

On July 30, 2018, a federal magistrate judge signed a warrant authorizing the search of Defendant's home. (Doc. No. 59-1.) The warrant also authorized the seizure of Defendant's "computers or storage media used as a means to commit" the offenses charged in this case, and searches of those devices for, among other things: "evidence of who used, owned, or controlled the [device] . . . such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, 'chat,' instant messaging logs, photographs, and correspondence." (*Id.*, pp. 6–9, 48.) Federal agents executed the warrant on August 2, 2018. Now-retired FBI Special Agent Christopher Avery was present during the search and testified at the hearing. Agent Avery served as a Special Agent with the FBI for twenty-three years. He functioned as the search team leader and seizing agent for the August 2, 2018, search of Defendant's home.

During the search, agents seized Defendant's cell phone, an iPhone X, and placed it in an evidence bag labeled "1B4." The phone and bag were admitted as exhibits at the hearing. Agent Avery testified that he labeled the evidence bag containing Defendant's iPhone X, and he identified his initials as still faintly visible on the bag. Defendant proffers he told agents on August 2, 2018, that the password to his iPhone X was "032889." That series of digits is also written on the bag. Also on August 2, 2018, Agent Avery surrendered the phone to the evidence control technician, which he testified was standard procedure. As part of his duties as seizing agent, Agent Avery completed a report called a "597." Agent Avery's 597 was admitted as evidence at the hearing. That report reflects seizure of an "Item #3," an iPhone X found in "Room O." Agent Avery briefly served as the case agent in this case, but retired in November 2019, at which time he testified the case would have been assigned to another agent.

At the hearing, one former and one current FBI employee testified concerning how the Bureau conducts digital forensic examinations and the tools they use to do so. They also testified about the Computer Analysis Response Team's, ("CART"), involvement with Defendant's iPhone X. Former Senior Examiner Victor Gibson Grose was employed with FBI CART in the Charlotte office from 2018 to 2021.¹ He testified that FBI CART is responsible for forensic extraction and analysis of devices. In Grose's role, he completed intake, trained other examiners, and completed forensic extractions and data analysis. Grose testified that while examiners occasionally completed forensic analysis on site, that process typically occurred at the FBI office.

During the relevant time, FBI CART in Charlotte was busy. That team was responsible for digital forensics within this District and outside it based on staffing needs, including due to a retirement in the Wilmington office and assistance needed in the Greenville office. Grose testified the office was not provided additional resources to handle this extra work. He testified that when he left the Charlotte office in 2021 two examiners remained. He further testified work priorities were determined based on whether there was an imminent threat of loss of life or limb, and at the direction of superiors.

On August 16, 2018, Grose charged Defendant's iPhone X out of evidence lockup. The evidence log, which was admitted as an exhibit during the hearing, does not note a reason why Grose charged out the device. (Doc. No. 62-1, p. 3.) He testified he charged it out for examination. Grose explained that the typical process when an examiner charges out a device for the first time is to check the physical state of the device and whether it is charged and/or powered on, determine the model, and determine whether an extraction is possible. Examiner Grose was unable to extract data from Defendant's iPhone X in 2018. He did not recall whether he tried the passcode written

¹ After transferring to the Raleigh office in 2021, Grose achieved the additional certification of Master Examiner.

on the evidence bag but believes he would have. He did not make the notations on the bag, consistent with Retired Agent Avery's testimony that Avery himself made the notations.

Grose also testified about a technology called Gray Key, which is a device and software formerly owned by the company GrayShift. GrayKey utilizes known software exploits to bypass security features—usually for Apple devices. The technology allows an examiner to extract the device's data, including by “brute force” if necessary. Grose further testified that GrayKey is constantly updating, and examiners periodically check out devices and plug them in to GrayKey to determine whether a new update allows access to a particular device. Grose testified that as GrayKey and other software identifies security holes, Apple updates its software. Therefore, GrayKey is constantly “playing catch up” with Apple. The FBI CART team in Charlotte acquired GrayKey sometime in 2020. Examiner Grose could not recall the exact date, but testified it was some time after the team resumed normal operations after the onset of the COVID-19 pandemic. GrayKey was not available to FBI CART in Charlotte when Grose first charged out Defendant's iPhone X in 2018. However, Defendant attached to his Reply brief a report by the Department of Homeland Security dated June 1, 2019, concerning GrayKey that notes the version of GrayKey available at that time primarily worked “as expected” on an iPhone X running iOS 11.3.1. (Doc. No. 64-2, pp. 7, 11–12.) At various times, FBI CART examiners have had access to other extraction software and hardware, namely Celebryte and 4PC. Grose testified Celebryte and 4PC require a device to be unlocked to perform an extraction.

Between January 31, 2020, and March 31, 2020, Examiner Grose again charged Defendant's iPhone X out of evidence. (Doc. No. 62-1, p. 2.) Grose was unable to perform an extraction on Defendant's iPhone X in 2020. The only documentary evidence of Examiner Grose's efforts to perform an extraction on Defendant's iPhone X in 2018 and 2020 is the evidence control

log. That document does not indicate why the device was charged out or any other information about Grose's efforts to perform an extraction on the phone.

Between February 10, 2021, and July 28, 2021, Examiner Grose again charged Defendant's iPhone X out of evidence. (Doc. No. 62-1, p. 2.) At this time, GrayKey was available to FBI CART in Charlotte. Using GrayKey, Examiner Grose was able to perform an extraction. He testified this extraction was limited to surface level data based on an iPhone state of "before first unlock." (Doc No. 62-3, p. 1.) During his testimony, Grose explained iPhones generally have three states with different levels of security: (1) "before first unlock;" (2) "after first unlock;" and (3) unlocked. He testified that an iPhone in a state of "before first unlock" may have recently been restarted or turned on and the bare minimum information is available to an examiner unencrypted. He further testified that an iPhone in a state of "after first unlock" has had the passcode entered at least once since its last restart and more—but not all—information is unencrypted and available. Finally, he explained a fully unlocked phone gives an examiner the capacity to complete a full extraction.

The GrayKey progress report Examiner Grose generated indicates the system retrieved 16.22 gigabytes of data from Defendant's iPhone X as a result of this extraction. (*Id.*, p. 2.) Examiner Grose could not testify about exactly what he did with Defendant's iPhone X during these five months beyond what is reflected in the GrayKey progress report. He testified charging out a device for multiple months was a common practice, and that examiners frequently charge out a batch of devices at a time and return them in a batch, as well. In December 2021, Former Examiner Grose transferred to the Raleigh office and had no further contact with Defendant's iPhone X.

FBI digital forensic examiner Lauren Haller also testified at the hearing. Haller joined the Bureau in June 2018 as an intern with the cyber squad, became a data analyst in the Raleigh office

in 2021, and joined the Charlotte office in April 2022. Haller testified that when she joined the Charlotte office, there were two other examiners. In February 2024, Haller charged Defendant's iPhone X out of evidence control at the request of the case agent. (Doc. No. 62-1, p. 2.) Before conducting the examination, Haller testified that she reviewed the 2018 warrant, but was not involved in any discussions concerning drafting a second affidavit. She plugged Defendant's iPhone X into the GrayKey software that was available at the time. GrayKey was able to complete the extraction without any "brute force" required. Haller could not recall the phone's lock state. The GrayKey progress report for her examination indicates the phone was in "no passcode set" mode. (Doc. No. 62-4, p. 1.) It also indicated the extraction size was 40.22 gigabytes of data. (Id., p. 2.) Haller's examination generated a report using Magnet Axiom. She compared the Magnet report to the Cellebrite report former Agent Grose created in 2021. In addition to containing more than twenty gigabytes of additional data, the Magnet report also included WhatsApp chats between Defendant and Bishop and Sumit Mittal. After she extracted the data, Haller created a form 302 detailing her work for the file. (Def. Ex. 2.) She testified it is standard practice to make similar notes to the file. Haller could not recall any further examinations of Defendant's iPhone X after February 2024 or any additional reports she created concerning this device.

Defendant moves to suppress the evidence gathered from Haller's 2024 search of his iPhone X under the Fourth Amendment, arguing the delay in extracting the data is unreasonable. The Government opposes the Motion, arguing the delay was justified by Apple's encryption protection, the availability of GrayKey, and staffing issues. Further, even if the search was unreasonable, the Government argues the good faith exception applies.

II. DISCUSSION

In the pleadings, the parties identify four issues: (1) whether Agent Haller's February 2024 search of Defendant's iPhone X was unreasonable under the Fourth Amendment; (2) whether the government's retention of Defendant's iPhone X for six years after the 2018 search was unreasonable under the Fourth Amendment; (3) whether the government complied with Rule 41 of the Federal Rules of Criminal Procedure; and (4) whether the government complied with the terms of the warrant. At the hearing, both parties focused their presentation of evidence and argument on Fourth Amendment reasonableness.

The Government did not act unreasonably in retaining Defendant's iPhone X during the pendency of its investigation and prosecution. Further, FBI CART did not act unreasonably in conducting the February 2024 extraction based on the manpower and technological resources available at the time. Therefore, suppression is inappropriate. Further, the Government did not violate Rule 41, which expressly permits later copying or review of electronic data seized pursuant to a warrant with no firm time limitation. The Government also did not violate Rule 41 by retaining Defendant's iPhone X, the return of which he never demanded under Rule 41(g).

A. Reasonableness of Retention and Search

Defendant argues the six-year delay between when officers seized Defendant's iPhone X and when Agent Haller successfully performed a full extraction of its data was unreasonable. The Government points to two justifications for the delay: the availability of technology that could get past Apple's encryption, and FBI CART Charlotte's workload and staffing.

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." U.S. Const. amend. IV. Generally, this means a search or seizure is unreasonable unless authorized by a warrant. United

States v. Brinkley, 980 F.3d 377, 383 (4th Cir. 2020). “[S]earches pursuant to a warrant will rarely require any deep inquiry into reasonableness, for a warrant issued by a magistrate normally suffices to establish that a law enforcement officer has acted in good faith in conducting the search.” United States v. Leon, 468 U.S. 897, 922 (1984) (cleaned up).

However, “A seizure that is ‘lawful at its inception can nevertheless violate the Fourth Amendment because its manner of execution unreasonably infringes possessory interests.’” United States v. Pratt, 915 F.3d 266, 271 (4th Cir. 2019) (quoting United States v. Jacobson, 466 U.S. 109, 124 (1984)). Generally, evidence seized in violation of the Fourth Amendment is subject to suppression under the exclusionary rule. See United States v. Calandra, 414 U.S. 338, 347–48 (1974); United States v. Perez, 393 F.3d 457, 460 (4th Cir. 2004). The overarching purpose of the rule is “to deter future unlawful police conduct.” Calandra, 414 U.S. at 347.

“The general touchstone of reasonableness which governs Fourth Amendment analysis . . . governs the execution of the warrant.” United States v. Ramirez, 523 U.S. 65, 71 (1998). It follows, therefore, that “[i]n the [warrant] execution context, as elsewhere, Fourth Amendment reasonableness kicks in.” Cybernet, LLC v. David, 954 F.3d 162, 168 (4th Cir. 2020). “[C]ourts agree that such review must occur within a reasonable amount of time to comply with the Fourth Amendment.” United States v. Cawthorn, 682 F. Supp. 3d 449, 457 (D. Me. 2023) (collecting cases). Even lengthy delays may be reasonable where the government presents a justification for the delay. Id. at 458 (collecting cases).

Defendant’s primary argument relies on Cawthorn. There, the court suppressed certain data from the defendant’s Instagram account. Id. at 457. Instagram produced the data to the Government pursuant to a warrant in December 2020. Id. at 454. Subsequently, investigators conducted several searches, including in March and June of 2023. Id. In Cawthorn, the Court concluded the

Government “[did] not justify its delay.” Id. at 458. Specifically, neither counsel nor any witness explained how the amount of evidence, complexity, workload of investigating agents, or any other factor prevented the Government from reviewing the defendant’s unencrypted Instagram data within a reasonable time². Id. Indeed, the record in Cawthorn indicated the Government only conducted further review of the available data in the days leading up to court deadlines. See id. at 459 (finding the Government “apparently only conducted further reviews . . . the day before its responses were due to certain pretrial motions . . . and . . . a few days after the most recent Motions Hearing”).

Here, the government points to the staffing and workload of FBI CART in Charlotte and the challenges presented by encryption to justify the delay. (Doc. No. 62, p. 14.) Former Agent Grose testified the FBI CART team in Charlotte was busy between 2018 and 2021. The team was assisting with work out of other Districts and was not provided additional resources to do so. When Grose left the Bureau in 2021, there were only two examiners in Charlotte. Based on Grose’s explanation of his attempts to extract data from Defendant’s iPhone X and the GrayKey technology, Apple’s encryption technology presented another source of delay. Other district courts have recognized this hurdle as a reasonable cause of delay. See United States v. Magana, No. 1:18-cr-00068, 2022 WL 4237547, at *6 (E.D. Cal. Sept. 14, 2022) (collecting cases concerning reasonable delay due to “encryption or inability to access a locked phone”); United States v. Este, No. 19-0711, 2020 WL 6075554, at *15 (S.D.N.Y. Oct. 14, 2020) (finding delay caused by encryption reasonable); United States v. Hansen, No. 18-00346, 2019 WL 5846879, at *11 (D.

² Defendant also argues Cawthorn supports suppression here because that Court noted “the Government essentially sat on a vast trove of personal data for over two years.” Cawthorn, 682 F. Supp. 3d at 459. But the Cawthorn court made this observation *after* having already determined the search was unreasonable—this language supported the Court’s reasoning why suppression was the appropriate remedy. Id.

Idaho Nov. 7, 2019) (finding a search reasonable given the volume of data and “the limited resources available to the Government”).

Defendant argues, based on the Homeland Security Report, that the GrayKey software was “available and fully vetted by the government long before the February 8, 2024, search of Mr. Banwari’s cell phone.” (Doc. No. 64, p. 5.) However, this argument does not account for Gray Key’s availability in the Charlotte office or staffing shortages in the Charlotte office. Ultimately, the question of reasonableness on these facts hangs on the credibility of the witnesses, particularly former examiner Grose. And the Court—having heard the evidence and observed the demeanor of the witnesses at the hearing—finds the Government’s explanation credible. United States v. Springer, 715 F.3d 535, 547 (4th Cir. 2013) (confirming a district court’s discretion to assess the credibility of witnesses and that such determinations are entitled to “due deference”).

Defendant appears to argue the Court should not credit the examiners’ testimony because Defendant told law enforcement the password to his phone. It is disputed whether that password worked. Even if it did, the record demonstrates it is Apple’s encryption technology—not any act of Defendant or the Government—that prohibited a full extraction until Haller successfully performed the extraction using GrayKey technology available in 2024. Finally, while there is no evidence Defendant affirmatively prevented law enforcement from accessing his iPhone X, whether Defendant caused the delay is not the question—it is whether the Government has presented evidence of a good faith justification for the delay. For the reasons set forth above, the Court concludes that it has done so.

Defendant’s request for an adverse inference because the government purportedly “lost or destroyed” relevant evidence—specifically, more detailed reports of Grose’s efforts to access Defendant’s iPhone X—is not supported by the record. See United States v. Johnson, 996 F.3d

200 (4th Cir. 2021) (considering whether an adverse inference was appropriate where the Government lost the victim’s cell phone). Rather, Grose’s testimony at the hearing demonstrates certain reports Defendant expected to exist were simply never created. While this may not reflect best practice—consistent with Haller’s testimony that she always writes a 302 to the file—it does not amount to “losing” or “destroying” evidence and the Court will not draw an adverse inference against the government on this basis.

At bottom, the six-year delay was lengthy, but it was not unreasonable under the facts and circumstances of this case, where the Government was unable to fully access the iPhone X’s data until at least three years after it was seized—perhaps more—and where workload and staff turnover caused delay.³

With respect to the Government’s retention of Defendant’s iPhone X, Defendant relies on United States v. Pratt, 915 F.3d 266, where the Fourth Circuit held the government’s 31-day delay in obtaining a warrant for the defendant’s cell phone—during which time the phone was in the Government’s possession—was unreasonable. However, that logic is inapplicable here. When the government seized Defendant’s iPhone X, agents did so in reliance on a warrant authorizing its search and seizure. And even in Pratt, the Fourth Circuit recognized that “overwhelmed police resources or other ‘overriding circumstances’ could justify extended delays.” Id. at 272 (quoting United States v. Mitchell, 565 F.3d 1347, 1353 (11th Cir. 2009)). In Pratt, the Court concluded the Government’s only justification was insufficient because “the agents failed to exercise diligence by spending a whole month debating where to get a warrant,” North Carolina or South Carolina, and it was “unlikely that the forum for a warrant would affect a later prosecution.” Pratt, 915 F.3d

³ In a footnote, Defendant attempts to preserve an argument that the 2022 search of his iPhone X was also unreasonable. (Doc. No. 59, p. 6 n.1.) For the same reasons set forth above with respect to the 2024 search, the Court concludes the 2022 search was reasonable.

at 272. Further, the search warrant in this case did not mandate return of the phone by any date certain, or even based upon a triggering event. Cf. Magana, 2022 WL 4237547, at *4 n.10 (concluding warrant required return of seized cell phone within ninety days of triggering condition, which never occurred). The Court concludes the Government did not violate the Fourth Amendment by retaining Defendant's iPhone X while its investigation and this case remained pending, and the warrant did not mandate it be returned.

B. Rule 41

The Court will briefly address whether the Government violated Rule 41 of the Federal Rules of Criminal Procedure, which provides:

A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information. Unless otherwise specified, the warrant authorizes a later review of the media information consistent with the warrant. The time for executing the warrant in Rule 41(e)(2)(A) and (f)(1)(A) refers to the seizure or on-site copying of the media or information, and not to any later off-site copying or review.
Fed. R. Civ. P. 41(e)(2)(B).

The Rule in its current form was first introduced in the 2009 Amendments. The Committee Notes to those Amendments explain “consideration was given to a national or uniform time period within which any subsequent off-site copying or review of the media or electronically stored information would take place.” Fed. R. Civ. P. 41 advisory committee’s note to 2009 Amendment. But the Committee rejected the proposed uniform time period because “[a] substantial amount of time can be involved in the forensic imaging and review of information.” Id.

The plain language of the Rule and the Committee’s intent, as expressed in the advisory note, is dispositive. The Court concludes the later search of Defendant’s iPhone X does not violate the letter or the spirit of Rule 41. During argument, defense counsel acknowledged the Rule does not impose a time requirement and properly focused on reasonableness, as addressed above.

With respect to the government's retention of the phone, Defendant acknowledges he did not make a demand for return of property. Federal Rule of Civil Procedure 41 sets forth the procedure by which he could do so. See Fed. R. Civ. P. 41(g). But Defendant made no such Motion, and the Court concludes the Government's retention of Defendant's iPhone X during the pendency of this investigation and prosecution of this case has not violated Rule 41.

C. Remaining Issues

At the hearing, Defendant did not press that the search exceeded the scope of the warrant. The Government argued the issue is so clear that he "could not." And Defendant's argument on this point in his pleadings is sparse. Further, the Court need not reach the parties' arguments concerning the good faith exception to the exclusionary rule because it has concluded the search complied with the Fourth Amendment and Rule 41 of the Federal Rules of Criminal Procedure.


III. CONCLUSION

In conclusion, nothing about Haller's 2024 search of Defendant's iPhone X was so unreasonable as to violate the Fourth Amendment or rebut the presumption of reasonableness that arises from the valid warrant in this case. And neither the government's retention or search of the phone violates Rule 41, particularly where Defendant never demanded return of the iPhone (and has not done so to this day). For all these reasons, the Court **DENIES** Defendant's Motion.

IT IS THEREFORE ORDERED that Defendant's Motion to Suppress, (Doc. No. 59), is **DENIED**.

IT IS SO ORDERED.

Signed: January 6, 2025


Frank D. Whitney
Senior United States District Judge

